

## 11. INTRODUCCIÓN A LOS CÓDIGOS LINEALES

Una de las aplicaciones más recientes del álgebra lineal es a la teoría de códigos, que trata el problema de representar información para facilitar su procesamiento, envío por diferentes canales y posterior recuperación. A grandes rasgos, la transmisión de información consta de los siguientes elementos:

- El **emisor** y el **receptor** del mensaje, que son respectivamente quien emite y recibe el mensaje.
- El **canal**, es el medio físico de transmisión por el que viajan las señales portadoras del mensaje.
- El **código**, es las distintas formas que puede tomar el mensaje para ser emitido. Cada uno de los elementos de un código se denomina **palabra código**. El lenguaje humano y la escritura pueden ser considerados códigos. Otros son el código Morse, el código de barras, el NIF, el ISBN usado en los libros, el ASCII usado en los ordenadores etc.

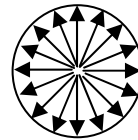
En general, cualquier medio tecnológico que transmita o almacene mensajes, como los ordenadores, las transmisiones vía satélite, los CD's, involucra al menos un código, y con frecuencia estos códigos están escritos con dos dígitos: 0 y 1.

Un **código sobre**  $\mathbb{Z}_2^n = (\{0, 1\})^n$  es un conjunto arbitrario de vectores del espacio vectorial  $\mathbb{Z}_2^n$  con el que se representa numéricamente la información.

Un buen código debería de ser capaz de recuperar un mensaje incluso en el caso de que en algún tipo de interferencia en el canal (lo que se denomina **ruido**) haya podido distorsionarlo. Un **error** será el cambio involuntario en una de las componentes de una palabra código.

### EJEMPLO 26

Se va a enviar a la Luna un pequeño artefacto de exploración que será manejado por control remoto desde la Tierra. El artefacto recibirá mensajes enviados por medio de un canal que transmite impulsos eléctricos de dos



voltajes distintos, que notamos por 0 y 1. Los mensajes que se quieren enviar son 16 posibles direcciones de movimiento. Se quiere obtener el menor valor de  $n$  para el que se puede construir un código sobre  $\mathbb{Z}_2^n$  con estas características, y estudiar qué ocurre si hay ruido en el canal de transmisión que altera uno de los dígitos.

**Solución:**

Se necesitan 16 palabras código distintas, el número de elementos de  $\mathbb{Z}_2^n = (\{0, 1\})^n$  es  $2^n$ , así que el menor  $n$  para el cual  $\mathbb{Z}_2^n$  tiene 16 elementos es:  $2^n = 16 \Rightarrow n = 4$ , y el código sería todo  $\mathbb{Z}_2^4$ :

$$\mathcal{C} = \left\{ p_1 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, p_2 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, p_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, p_4 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}, p_5 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, p_6 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix}, p_7 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \right.$$

$$p_8 = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, p_9 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, p_{10} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, p_{11} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}, p_{12} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix},$$

$$p_{13} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, p_{14} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, p_{15} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \end{pmatrix}, p_{16} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \Big\}$$

Si se envía por ejemplo la palabra código  $p_{10} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$  y por ruido en el canal se recibe  $\begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}$ , al

ser la palabra recibida una palabra código (exactamente  $p_{14}$ ), podría perfectamente haber sido la palabra enviada. Se deduce que con este código no se puede detectar que ha habido un error de transmisión, y mucho menos corregirlo.

### 11.1. CÓDIGOS LINEALES

Dados dos enteros positivos  $k$  y  $n$  con  $0 < k \leq n$ , un **código lineal**  $(n, k)$  es cualquier subespacio vectorial de dimensión  $k$  del espacio vectorial  $\mathbb{Z}_2^n$ . Todas las posibles combinaciones lineales de los  $k$  elementos que tiene una base de un código lineal  $(n, k)$  son en total  $2^k$  palabras que forman el código.

#### EJEMPLO 27

Obtener una base del código lineal, conocido como **código de Hamming**  $(7, 4)$ , y definido por

$\mathcal{C} = \{x \in \mathbb{Z}_2^7, \text{tales que } Hx = \mathbf{0}\}$ , siendo  $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ , y calcular cuántas

palabras distintas tiene este código.

**Solución:**

Dado que  $\text{rango}(H) = 3$ , se tiene que la dimensión del subespacio vectorial  $\mathcal{C}$  es:  $\dim(\mathcal{C}) = 4$ . Para obtener una base del espacio solución, se hacen operaciones elementales en las filas de la matriz, teniendo en cuenta que todas las operaciones se realizan módulo 2:

$$H \sim \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \Rightarrow$$

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} \in \mathcal{C} \Leftrightarrow \begin{cases} x_1 = \alpha + \beta + \delta \\ x_2 = \alpha + \gamma + \delta \\ x_3 = \alpha \\ x_4 = \beta + \gamma + \delta \\ x_5 = \beta \\ x_6 = \gamma \\ x_7 = \delta \end{cases} \Leftrightarrow \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + \gamma \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + \delta \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Una base de  $\mathcal{C}$  es por tanto  $\mathcal{B}_{\mathcal{C}} = \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$ . Las combinaciones lineales de

estos cuatro elementos con los coeficientes 0 y 1 son  $2^4 = 16$ , que es el número total de palabras código.

### 11.1.1. DEFINICIÓN

Sea  $\mathcal{C} = \{\mathbf{x} \in \mathbb{Z}_2^n, \text{tales que } H\mathbf{x} = \mathbf{0}\}$  el código lineal  $(n, k)$  definido como el espacio de soluciones de un sistema de ecuaciones lineales homogéneo. La matriz de coeficientes del sistema  $H \in \mathcal{M}_{m \times n}$  recibe el nombre de **matriz de paridad** del código  $\mathcal{C}$ .

## 11.2. DETECCIÓN Y CORRECCIÓN DE ERRORES EN CÓDIGOS LINEALES

### 11.2.1. TEOREMA

Si  $\mathcal{C}$  es un código lineal  $(n, k)$  cuya matriz de paridad  $H \in \mathcal{M}_{m \times n}$  no contiene una columna de ceros ni dos columnas iguales, entonces el código  $\mathcal{C}$  es capaz de corregir un error.

**Demostración.**

Para cada  $i$  desde 1 hasta  $n$  sea  $\mathbf{e}_i$  el vector de  $\mathbb{Z}_2^n$  cuyas componentes son todas cero menos la componente  $i$  –ésima que es uno, y sea  $B_c^n = \{\mathbf{e}_1, \dots, \mathbf{e}_n\}$  la base de  $\mathbb{Z}_2^n$  formada por estos vectores. Se tiene entonces que  $H\mathbf{e}_i = \mathbf{c}_i$ , siendo  $\mathbf{c}_i$  la columna  $i$  –ésima de la matriz  $H$ .

Sea  $\mathbf{x} \in \mathcal{C}$  una palabra código enviada, por ser palabra código  $\mathbf{x}$  verifica que  $H\mathbf{x} = \mathbf{0}$ .

Sea  $\mathbf{y} = \mathbf{x} + \mathbf{e}_i$  la palabra recibida, en la que la componente  $i$  –ésima de  $\mathbf{x}$  ha sido alterada.

Entonces se tiene que: 
$$H\mathbf{y} = H(\mathbf{x} + \mathbf{e}_i) = H\mathbf{x} + H\mathbf{e}_i = \mathbf{0} + \mathbf{c}_i = \mathbf{c}_i$$

Puesto que  $H$  no tiene ninguna columna de ceros, se tiene que  $H\mathbf{y} = \mathbf{c}_i \neq \mathbf{0}$ , por lo que se detecta que ha habido un error en la transmisión.

Además  $H\mathbf{y} = \mathbf{c}_i$ , y  $H$  no tiene dos columnas iguales, por lo que se puede determinar el valor de la coordenada modificada  $i$ , localizando la posición que ocupa la columna  $H\mathbf{y}$  en la matriz  $H$ . Por tanto el error puede ser corregido.

### 11.2.2. PROCESO PARA DETECTAR Y CORREGIR UN ERROR

Sea  $\mathcal{C}$  un código lineal  $(n, k)$  con matriz de paridad  $H \in \mathcal{M}_{m \times n}$  que no contiene una columna de ceros ni dos columnas iguales y sean  $\mathbf{x}$  la palabra enviada e  $\mathbf{y}$  la palabra recibida, entonces:

1. Si  $H\mathbf{y} = \mathbf{0}$ , entonces no ha habido error de transmisión y se tiene que  $\mathbf{x} = \mathbf{y}$ .
2. Si  $H\mathbf{y} \neq \mathbf{0}$  entonces es  $H\mathbf{y} = \mathbf{c}_i$  siendo  $\mathbf{c}_i$  la columna  $i$  –ésima de la matriz  $H$ . Se tiene que la palabra código enviada es  $\mathbf{x} = \mathbf{y} + \mathbf{e}_i$ .

#### EJEMPLO 28

Usando el código de Hamming  $(7, 4)$  con matriz de paridad  $H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$ ,

se han recibido las siguientes palabras:

$$\mathbf{y}_1 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \mathbf{y}_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix}, \mathbf{y}_3 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

determinar si ha habido un error de transmisión y en caso afirmativo corregir dicho error.

**Solución:**

Se calcula el producto de  $H\mathbf{y}_i$ :  $H\mathbf{y}_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ ,  $H\mathbf{y}_2 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ ,  $H\mathbf{y}_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ ,

De donde se deduce que  $\mathbf{x}_1 = \mathbf{y}_1 + \mathbf{e}_4 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$ ,  $\mathbf{x}_2 = \mathbf{y}_2 + \mathbf{e}_7 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}$  y  $\mathbf{x}_3 = \mathbf{y}_3$ , en este

último no ha habido error de transmisión.